



The Latest Scams Circulating the Consumer World.

Receive Free Lesson Plans
and More:



November 2009

Use Caution When Purchasing With a Debit Card

The Hook

Purchasing items online and in retail stores using a debit card.

The Scam

The most recent elaborate fraud involves the theft of debit card data. Enterprising and clever cyber-criminals have recently become adept at stealing supposedly confidential data from retail stores and banks.

Play it Safe

Do not use debit cards to purchase items over the internet. Also, use caution when using debit cards in retail stores.

The Whole Story

The latest scheme involves cyber-criminals living in Russia, Estonia and Moldova. Three fraudsters hacked into the Royal Bank of Scotland's World Pay computer network and cracked the encryption codes protecting account numbers and pins for 44 prepaid payroll accounts. Many companies have utilized such accounts to distribute salaries to their employees via debit cards. Their employees then can use their debit cards at ATM machines and various stores to serve as cash where they withdraw their pay and never run the risk of an overdraft.

In this particular case, these cyber-thieves hacked the bank system, increased the payroll account limits, then arranged to have the stolen account numbers embedded in the magnetic stripes of blank payment debit cards. The scheme got extremely creative and complex when they hired an army of cashiers in 280 cities worldwide. In just 12 hours, using the counterfeit debit cards, the cashiers withdrew over \$9 million from more than 2,000 ATMs in the United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan and Canada. The cashiers that were hired in the 280 cities worldwide took a piece of the action. It is believed they were paid up to 30% of the amount debited simply for inserting the cards and withdrawing the cash. They then remitted the cash to the three creative fraudsters in Eastern Europe.

The level of coordination required by the three fraudsters and the various cashiers was described as "staggering" by the officials involved in unwinding the plot. A leading security analyst claims that the ringleaders probably spent months on internet forums recruiting card counterfeiters and cashiers and plotting a fast moving wave of withdrawals that amounted to a surprise 12-hour attack on the bank's account. "The element of surprise allows you to do a tremendous amount of damage in a short span of time", says Uri Rivner, a security analyst. "It's like an Al Qaeda strategy of multiple attacks in a single day" to spread fear and panic.

Lesson

The lesson for debit card users is to never, never use your debit card to purchase products over the internet, for the simple reason that you don't have any protection in the event of a fraud. Once the cash is taken from your account, it's gone forever. But if you pay with a credit card you have 30 days in which to analyze your account and have protections granted to you by the credit card companies to challenge any dubious charge that you did not make. These same protections are not available to debit cards.

When using your debit card to pay for things like meals at a restaurant and for goods at a retail store, use extreme caution. A clerk can watch your pin number being put in, ask to see your card, pretend to examine it out of your sight, and then switch it with an identical looking card, but one that has someone else's name on it. If you ever hand over your debit card to a clerk, be sure you check the name on it when you get it back.

There is one other gimmick to watch out for. Many retail outlets charge a fee for the use of your debit card, a fee that is hidden and can cause you to overdraft your account! Even worse, some retail outlets may delay the charge for a couple of days, meaning if you check your bank balance over the internet, you may be deceived into thinking there is more there than there really is!